(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4775011号
(P4775011)

(45)発行日　平成23年9月21日(2011.9.21)　(24)登録日　平成23年7月8日(2011.7.8)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330E
G06F 21/24	(2006.01)	G06F	12/14	530D
H04L 9/32	(2006.01)	H04L	9/00	673C

請求項の数 2　(全 10 頁)

(21)出願番号　特願2006-28064(P2006-28064)
(22)出願日　平成18年2月6日(2006.2.6)
(65)公開番号　特開2007-207148(P2007-207148A)
(43)公開日　平成19年8月16日(2007.8.16)
審査請求日　平成20年6月13日(2008.6.13)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100109667
弁理士　内藤　浩樹
(74)代理人　100109151
弁理士　永野　大介
(74)代理人　100120156
弁理士　藤井　兼太郎
(72)発明者　松下　尚史
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

審査官　深沢　正志

最終頁に続く

(54)【発明の名称】パスワード機能を備えた情報処理装置

(57)【特許請求の範囲】
【請求項１】
パスワードを入力する第１の文字入力手段と、
記録媒体の着脱やボタンの入切のような２値以上の状態の検出が可能な少なくとも１つ以上の状態入力手段と、
前記１つ以上の状態入力手段からの各々の状態信号を検出し、特殊な文字コードに変換を行なう第２の文字入力手段と、
前記第１および第２の文字入力手段からの文字入力状況を使用者に提示する表示手段と、
前記第１および第２の文字入力手段より入力された文字を所定のパスワードと照合するパスワード照合手段と、
を備え、
前記表示手段は、前記第２の入力手段により入力された特殊文字に対しては規定の属性情報を付加し、使用者に対して特殊文字の聴視による確認または隠蔽をすることを可能とし、
前記パスワード照合手段は、前記第１の入力手段により入力された文字と、前記第２の入力手段により入力された特殊文字とを、所定の方法で合成または分離または加工し、所定のパスワードと照合して正誤判定を行なうことを特徴とするパスワード機能を備えた情報処理装置。
【請求項２】
前記１つ以上の状態入力手段の少なくとも１つは、情報処理装置内の通常の使用者には操

作し得ない部位に設置され、
前記パスワード照合手段は、前記通常操作の不可能な部位に配置された状態入力手段を含む１つ以上の状態入力手段の検出した状態信号が、通常の使用者によらないと判定できる所定の入力条件を満たした場合、第１の文字入力手段から入力された文字と、前記第２の文字入力手段から入力された特殊文字とを、所定の方法で合成または分離または加工し、所定のパスワードと照合して一致した場合には、前記情報処理装置に予め設置された所定の組み込み機能を起動するようにしたことを特徴とする請求項１に記載のパスワード機能を備えた情報処理装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、パーソナルコンピュータ（以下「ＰＣ」）を代表とする情報処理装置のセキュリティ機能に関する。
【背景技術】
【０００２】
近年、ノート型ＰＣのような携帯型の情報処理装置が一般に広く普及し、容易に屋外にそれらを持ち出せるようになった反面、それらの盗難、そして内部に記録された情報が漏洩する事件が多発し社会問題化している。このような課題に対して、一般に最近のＰＣにはセキュリティ機能を付加していることは衆知の事実である。
【０００３】
例えばＰＣの不正使用を防止するために、その起動時にはパスワードを入力、照合しないとオペレーティングシステム（ＯＳ）が起動せずＰＣ自体の起動を拒否し、また個別情報へのアクセス時にはユーザーＩＤ、パスワードの正誤判定を行ない、データへのアクセス制御を行うのが一般的である。しかし、パスワードは一定桁の英数字または記号からなるために、英数字を変化させながら繰り返しパスワードを入力して行けば、いずれは正しいパスワードと一致することとなる。このとき、使用者のパスワード入力操作を不正に監視されていた場合、ディスプレイへの入力状況の表示やキーボードの操作状況などからパスワードの文字数や構成する文字を推測され、少ない試行回数でパスワードの特定ができてしまう。従ってパスワード漏洩の可能性は依然として高く、単にパスワード判定ステップを設けても個別情報への不正アクセスを有効に防止することができない。
【０００４】
図５は従来技術である特許文献１に係るＰＣの不正アクセス防止システムの動作を示すフローチャートである。
【０００５】
まず、ステップＡでは、使用者がＰＣの電源のＯＮを行う。ステップＢでは、ＰＣのパスワード確認処理部が、ＯＳを起動する前に、パスワード入力画面をディスプレイ装置に表示せしめ、使用者にパスワードの入力を促す。ここで、使用者はパスワードを入力装置であるキーボードから入力する。入力されたキーコードは、改行キーが来るまで、１文字毎にパスワード確認処理部の一時的な入力バッファに蓄えられ、入力された状況が使用者に分かるようにディスプレイ装置に表示される。但し、パスワードそのものが表示されないように”＊”などの別の記号に置き換えた上で表示されるのが一般的である。
【０００６】
上記入力要求により、使用者がキーボードからパスワードを入力したならば、ステップＣにて、パスワード確認処理部は、上記入力されたパスワードを予め設定されたパスワードと照合し、上記パスワードが不正な場合は、ステップＤにて、パスワード確認処理部がディスプレイ装置上に警告メッセージを表示した後、警告メッセージの表示回数のカウンタをカウントアップし、ステップＦにて、警告メッセージの表示回数が２回までならステップＢに戻して、再度、パスワードの入力を促す。あるいはステップＦにて、上記入力されたパスワードがキーボードから入力された３回目の不正なパスワードである場合、パス

ワード確認処理部はＰＣの電源をＯＦＦにする。ステップＣにて、パスワードの照合の結果が正しいならば、ステップＥにてＯＳの起動を行う。

【０００７】

以上説明したように、ＯＳでは防止できなかったＰＣへの不正なアクセスをＰＣの電源投入段階で防止することが可能となる。

【特許文献１】特開２００１－２７９１１号公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

しかしながら、上記従来の構成ではセキュリティ機能としては十分とは言えない。

【０００９】

特許文献１の従来の技術では、一旦このＰＣ上でパスワード設定をすればＰＣ起動時にこのパスワードを正しく入力しない限り複数回の試行で電源が切れるため、結果的にＨＤＤなどの記憶媒体の内容を読み出すことは確かに不可能である。

【００１０】

しかし、この従来技術ではパスワード入力の複数回の試行で電源が切れるとは言え、ディスプレイへの表示状況や使用者のキーボード操作を監視されることによりパスワードの文字数や構成文字の推測、漏洩は不可能ではなく、パスワードの解読によってＰＣの起動が可能となり、ＨＤＤ内に記録したデータを不正に読み出すことは依然として可能である。昨今、このような不正監視によるパスワードや暗証番号の漏洩は、銀行でのＡＴＭ利用時での被害例も報道されており、パスワード入力操作そのものにも注意していかなければならない。

【００１１】

一方、使用時のセキュリティを強固にすると実際の使用時や修理の際に支障がでることがある。

【００１２】

例えば、長く複雑なパスワードは強固であるが使用者が忘れてしまうとＰＣそのものを正規の使用者自身が使用できなくなる。また、セキュリティ設定をされたまま、装置の故障などでその修理を行なう場合、修理作業者は正規の使用者のパスワード情報を入手しセキュリティ設定を解除しておかないと、例え正規の修理であってもＰＣの起動が行なえないために修理作業や確認作業に支障が発生することがある。このようにセキュリティの強化、確保と修理作業とは一般的に両立が困難な課題である。

【００１３】

本発明は上記従来の課題を解決するもので、単純にパスワード入力の際のキーボード操作を不正に監視されたとしても容易に推測されないセキュリティ機能を提供するとともにパスワードの忘却や修理上の課題を解決する方法を提供することを目的とする。

【課題を解決するための手段】

【００１４】

本発明の請求項１に記載の発明は、

パスワードを入力する第１の文字入力手段（例えば図１のキーボード１１３）と、

記録媒体の着脱の検出やボタンの入切のような２値以上の状態の検出が可能な少なくとも１つ以上の入力手段（例えば図１のＦＤＤ１０９の出し入れを検出するＦＤＣ１０８）と、

前記１つ以上の入力手段からの各々の記録媒体（例えばＦＤＤ１０９）の着脱信号やタッチパッドの左右ボタン各々の入切状態信号を検出し、特殊な文字コードに変換を行う第２の文字入力手段と、

前記第１および第２の文字入力手段からの文字入力状況を使用者に提示する表示手段と、

前記第１および第２の文字入力手段より入力された文字を所定のパスワードと照合するパスワード照合手段と、

を備え、

前記表示手段は、前記第２の入力手段により入力された特殊文字に対しては規定の属性情報を付加し、使用者に対して特殊文字の聴視による確認または隠蔽をすることを可能とし、前記パスワード照合手段は、前記第１の入力手段により入力された文字と、前記第２の入力手段により入力された特殊文字とを所定の方法で合成または加工し、所定のパスワードと照合して正誤判定を行なうことを特徴とするパスワード機能を備えた情報処理装置としたものであり、

第１の文字入力手段でのパスワード入力に加えて、第２の文字入力手段による特殊文字を混ぜてパスワードを構成することによりパスワードそのものを強化する。たとえ第１の文字入力手段での操作を不正に監視されたとしても、第２の文字入力手段により一般に文字入力とはみなされないような操作を混ぜて文字を入力するため、パスワードを構成する文字の推測は困難である。さらには特殊文字の入力状態の表示を制限することを可能にするので、表示装置の不正監視に対する防御も強化できる。

【００１５】

これによりセキュリティをより強固なものにすることができる。

【００１６】

本発明の請求項２に記載の発明は、

前記１つ以上の状態入力手段の少なくとも１つは、例えば図１におけるマザーボード１０１上のジャンパースイッチ１１９のように情報処理装置内の通常の使用者には操作し得ない部位に設置され、前記パスワード照合手段は、前記通常操作の不可能な部位に配置された状態入力手段を含む１つ以上の状態入力手段の検出した状態信号が、通常の使用者によらないと判定できる所定の条件を満たした場合、第１の文字入力手段から入力された文字と第２の文字入力手段から入力された特殊文字とを、所定の方法で合成または分離または加工し、所定のパスワードと照合して一致した場合には、前記情報処理装置に予め設置された所定の組み込み機能を起動するようにしたことを特徴としたパスワード機能を備えた情報処理装置であり、

修理作業者のみが通常の使用者には操作し得ない部位に設置されたボタンやジャンパーの入切の状態信号を操作し、それらの状態信号が通常使用者には入力し得ない所定の条件を満たした場合で、かつ、第１および第２の所定のパスワードに各々一致した場合には、装置内に予め組み込まれた修理作業者向けの特殊機能を起動するようにする。この特殊機能では例えばセキュリティ設定をバイパスして装置を起動し、修理内容の動作確認ができるように設定しておく。

【００１７】

これにより、修理作業者は使用者のパスワード情報を知ることなく、所望の修理作業が可能となり、セキュリティ強化ともに修理性の向上も図ることができる。

【発明の効果】

【００１８】

以上のように、本発明によれば、キーボードのような通常の入力手段ではない特殊な操作からなる第２の文字入力手段を用いてパスワードを構成し、パスワード構成文字の推測を困難にしてセキュリティをより強固なものにすることができるとともに、第２の文字入力手段を構成する一部の状態入力手段を通常使用状態から隠して運用することにより修理作業にも支障のない情報処理装置を提供することができるようになる。

【発明を実施するための最良の形態】

【００１９】

以下、本発明を実施するための最良の形態について図１から図４を用いて説明する。

【００２０】

（実施の形態１）

図１は実施の形態１に係る一般的なＰＣのハードウエア構成図である。

【００２１】

図１において１０１はマザーボードであり、ＰＣを構成する主要なパーツを固定したり装着したりするためのパーツである。１０２はＣＰＵ（中央演算処理装置）、１０３，１

０４はチップセットと呼ばれノースブリッジ１０３はＣＰＵ１０２とメモリ、グラフィックチップ１２１の間を流れるデータを制御する。液晶ディスプレイ１２２はグラフィックチップ１２１を介してノースブリッジからの映像信号を表示する。サウスブリッジ１０４は、ＨＤＤ１０６，ＣＤ／ＤＶＤドライブ１０７をつなぐＡＴＡ（ＩＤＥ）インターフェース１０５、キーボードやマウスのインターフェース１１２、周辺デバイス（ＳＤコントローラー１１０やＬＡＮ、サウンドデバイスなど）、その他のインターフェース間を流れるデータの制御を行う。１１８は不揮発性のフラッシュメモリであり、ＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ／Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）と呼ばれるＰＣに接続されているＨＤＤ１０６やＣＤ／ＤＶＤ１０７、ＦＤＤ１０９（フロッピー（登録商標）ディスクドライブ）、ＦＤＣ１０８（フロッピー（登録商標）ディスクドライブコントローラ）などのディスクやキーボード、グラフィックチップなどのデバイスをコントロールするプログラム群が組み込まれている。ＢＩＯＳはユーザーによりＰＣの起動直後に所定のキーを押すことによりセットアップメニューを呼び出し、設定内容を変更することができる。設定した内容はサウスブリッジ１０４内のＣＭＯＳ領域にあるＣＭＯＳ１１６に記憶し、コイン電池１１７でバックアップするので電源を切っても保持される。

【００２２】

１１９はジャンパースイッチであり、マザーボード１０１上に設置され、サウスブリッジ１０４のＧＰＩＯピン１２０に接続され、ＢＩＯＳを経由してスイッチの設定状態を読み出すことができるようになっている。

【００２３】

１１５はＲＴＣ（リアルタイムクロック）であり、電源が切られている間も内蔵電池から電源供給を受け、ＯＳは起動時にリアルタイムクロックから日時を取得する。

【００２４】

１１３は文字入力のためのキーボード、１１４はノートパソコンで採用されているポインティングデバイスであるタッチパッドである。また１１１は外部記憶媒体である半導体メモリ（ＳＤカード）である。

【００２５】

以上のように構成されたＰＣに関して、本発明に掛かる第１の文字入力手段はキーボード１１３である。第２の文字入力手段は、ＦＤＤ１０９の出し入れ、ＳＤカード１１１の出し入れ、タッチパッド１１４の左右ボタンの押し放し操作、および装置の筐体からの取り出さなければ操作が出来ないマザーボード１０１上の部位に設置されたジャンパースイッチ１１９のピン状態を検出する各状態入力手段と、それら各状態入力手段からの状態信号を検出し特殊な文字コードに変換する制御プログラムを有するＢＩＯＳとにより構成される。これら第１および第２の文字入力手段からの文字入力状況は、液晶ディスプレイ１２２を表示手段として、図２に示すように表示される。

【００２６】

図２（ａ）はパスワードの入力画面の一例であり、通常のキーコードも特殊コードも区別なくパスワードを構成する文字を全て＊に置き換えて表示している。キーボードから入力された文字は大文字小文字を含む英数字および記号であり、ＡＳＣＩＩコードで表現すると１６進数で２０ｈから７Ｅｈの範囲となるが、特殊コードはその他の範囲にマッピングされているものとする。この場合、文字コードの区別なく全て＊で表示するため、使用者は特殊コードが入力できたことは確認できるが、第三者にはどちらの入力手段を用いたのかは表示上から推測ができないという利点がある。

【００２７】

図２（ｂ－１）、（ｂ－２）はキーボード以外の入力手段から得られた特殊コードを通常文字と区別して表示する場合の例であり、（ｂ－１）の場合は、特殊コードは全て別の色の＊で表示している（色の違いは下線付きの＊で示している）。また（ｂ－２）の場合は特殊コード毎に色や文字の形を変えて表示している。このように通常のキーコードとは表示を変えることにより使用者には特殊操作が有効に作用したことを確認させることができる。しかしながらキーボード以外の入力があったことが推測される可能性があるため、

図２（ａ）に比べてセキュリティ的には弱い。

【００２８】

図２（ｃ）は、これら特殊コードは入力可能であるが表示をしない例である。この場合、特殊コードの表示はしない代わりに入力されたことをブザーなどの音で知らせるようにしておけば、使用者は入力の確認が可能であるとともに、特殊コードの入力状態は画面に表示されないので操作を盗み見られてもパスワードの文字数や構成文字を推測される危険は少ない。これら特殊コードの表示方法はＢＩＯＳのセットアップメニューで選択可能なように構成している。

【００２９】

図３は、使用者がＰＣの電源を投入してからパスワード認証を行ないＯＳを起動するまでの操作のフローを示している。

【００３０】

ステップＳ０１で電源を投入すると、ステップＳ０２において図２に示すようなパスワード入力画面になる。ここで使用者は図１に示すキーボード１１３を第１の文字入力手段としてパスワードを１文字ずつ入力する。またキーボード１１３からの文字入力の合間にタッチパッド１１４の左右のボタン、ＦＤＤ１０９の抜き差し、ＳＤカード１１１の抜き差しを行なう。これらが第２の文字入力の操作であるが、このうちどれが特殊コードの入力操作に該当するか、あるいは操作の順番によってどのような特殊コードに変換するかは予めＢＩＯＳセットアップメニューで設定するようにしておく。そうすることによりキーボード１１３の操作やディスプレイ１２２の表示状態を盗み見られたからといって直ちにパスワードの推測や漏洩の危険にはつながらない。Ｓ０３でキー入力でない場合は、Ｓ０５で特殊操作を検出し、Ｓ０６で該当する特殊コードに変換する。このとき、各操作に対して、例えばＳＤカード１１１の挿入は８１ｈ、抜きだしは８２ｈというように別々の特殊コードを割り当ててもよいし、例えばＳＤカード１１１の挿抜もＦＤＤ１０９の挿抜も９０ｈというように特殊操作全てに同じ特殊コードを割り当てるとしてもよい。特殊操作毎に異なるコードを割り当てる場合は操作の順序関係を重視したパスワードとなり、一方同じコードを割り当てる場合は特殊操作の順には無関係なパスワードとなる。

【００３１】

さらにＳ０７において、セットアップメニューで予め選択した方式で特殊文字の文字表示情報を付加し、Ｓ０８で入力バッファを更新した後、パスワード入力状態の表示を更新する。Ｓ０３でキーボードからの入力の場合、さらにＳ０４において改行キーでない文字コードの場合は、表示属性は付加しないで入力バッファを更新し、＊を表示するようにする。またＳ０４において、改行キーであった場合には入力終了処理Ｓ０９に移行する。このとき、第１の文字入力手段で入力されたパスワードと第２の文字入力手段で入力されたパスワードは入力バッファに時系列に格納されている。

【００３２】

Ｓ１０はパスワード照合手段での判定処理である。パスワード照合手段においては、入力バッファに時系列に格納された文字コードを所定の手順で合成または加工を行ない、予め設定されたパスワードとの正誤判定を行なう。このとき、入力バッファ中にキーコードと特殊コードが所定の順でなければ正しくないと判定してもよいし、キーコードと特殊コードは分離して考え、別々に正誤判定するとしてもよい。

【００３３】

Ｓ１０で正しいと判定された場合は、Ｓ１２でＯＳの起動を行ない、誤りと判定された場合は、Ｓ１１で警告メッセージを表示し、誤りの回数に応じて電源をオフする（Ｓ１４）かまたはＳ０２に戻るようにする。

【００３４】

図４は、修理作業者が修理作業を行ない動作確認をする際の操作フローを示す。

【００３５】

修理作業者は、装置本体を分解し、マザーボード１０１上のジャンパースイッチ１１９を所望の入力値になるように変更してからＳ０１で電源を投入する。特殊コードを含むパ

スワード入力操作Ｓ１００は図３と同様である。ジャンパースイッチ１１９の入力値が所定の入力値になっている場合は、Ｓ２０において修理機能選択の状態信号が含まれると判定され、修理機能の起動判定処理Ｓ１０２に移行する。

【００３６】

なお、ジャンパースイッチ１１９の入力値が所定の入力値になっていない場合には、図３に示す通常のＰＣ起動としてパスワードを入力し、図３の波線内Ｓ１０１の処理が行われる。

【００３７】

Ｓ１０２でのパスワード照合手段ではＳ２１からＳ２３で示すように入力バッファ中に時系列で入力されたパスワードキーコードと特殊コードとを分離して照合するフローを例示している。Ｓ２１ではそれぞれのコードを分離し、Ｓ２２では特殊コードからなるパスワードを複数ある修理機能から特定の１つを選択するためのＩＤとし、キーコードからなるパスワードはその修理機能の起動のためのパスワードとみなして（Ｓ２３）、Ｓ２４において正誤判定を行ない、Ｓ２５で該当する修理機能を起動するように修理ユーティリティに指示し、修理完了後はＰＣを電源オフまたは再起動する（Ｓ２６）。

【産業上の利用可能性】

【００３８】

本発明にかかる情報処理装置は、キーボードのような通常の入力手段ではない特殊な操作からなる第２の文字入力手段を用いてパスワードを構成し、パスワード構成文字の推測を困難にしてセキュリティをより強固なものにすることができるとともに、第２の文字入力手段を構成する一部の状態入力手段を通常使用状態から隠して運用することにより修理作業にも支障がなくなり、パーソナルコンピュータを代表とするセキュリティ機能を具備すべき情報処理装置として好適である。

【図面の簡単な説明】

【００３９】

【図１】本発明の実施の形態１に係る一般的なＰＣのハードウエア構成図

【図２】（ａ）パスワードの入力画面を示す図（通常）、（ｂ－１）（ｂ－２）パスワード入力画面を示す図（特殊コード表示の場合）、（ｃ）パスワード入力画面を示す図（特殊コード非表示の場合）

【図３】本発明の実施の形態１に係る通常使用者のおける操作フローチャート

【図４】本発明の実施の形態１に係る修理作業者における操作フローチャート

【図５】従来技術である特許文献１に係るコンピュータの不正アクセス防止システムの動作を示すフローチャート

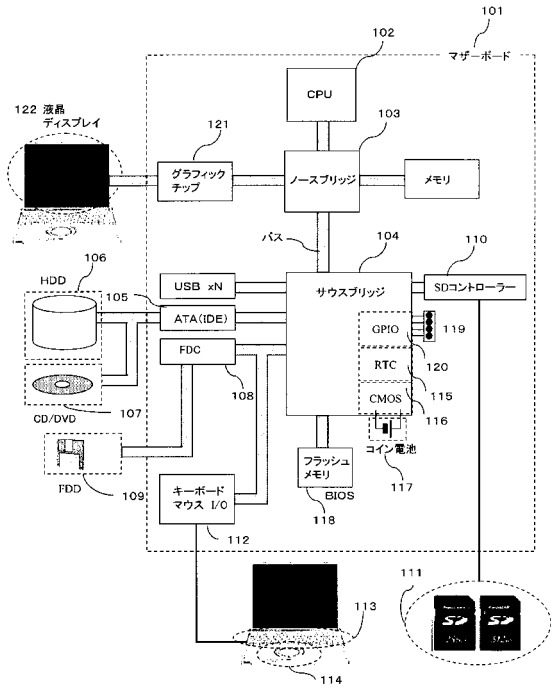
【符号の説明】

【００４０】

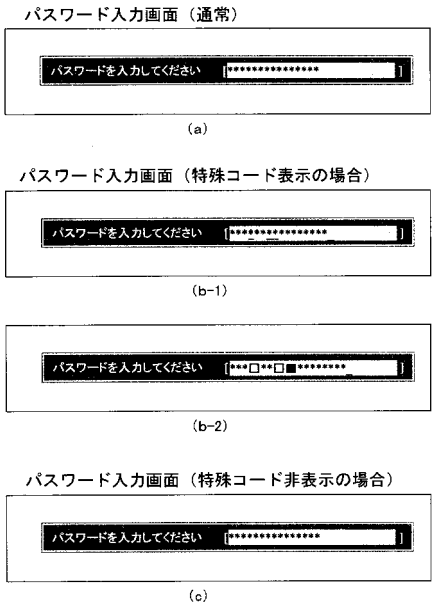
１０１　マザーボード
１０２　ＣＰＵ
１０３　ノースブリッジ
１０４　サウスブリッジ
１０５　ＡＴＡ（ＩＤＥ）インターフェース
１０６　ＨＤＤ（ハードディスクドライブ）
１０７　ＣＤ／ＤＶＤドライブ
１０８　ＦＤコントローラー
１０９　ＦＤドライブ
１１０　ＳＤコントローラー
１１１　ＳＤカード
１１２　キーボード、マウスＩ／Ｏコントローラー
１１３　キーボード
１１４　タッチパッド
１１５　ＲＴＣ（リアルタイムクロック）

１１６　ＣＭＯＳ
１１７　コイン電池
１１８　フラッシュメモリ
１１９　ジャンパースイッチ
１２０　ＧＰＩＯ

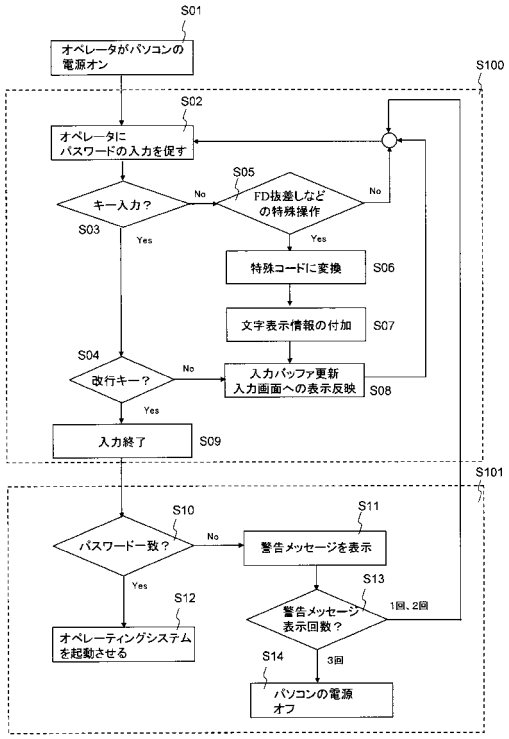
【図１】



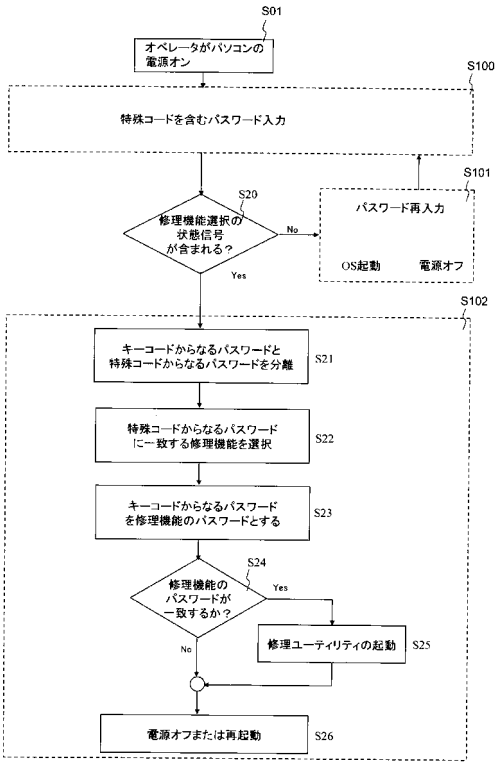
【図２】



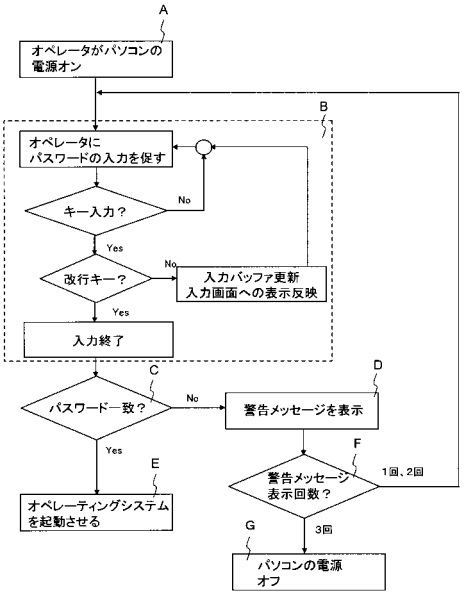
【図３】


S01
オペレータがパソコンの電源オン
S100
S02
オペレータにパスワードの入力を促す
S05
FD抜差しなどの特殊操作
No
キー入力？
S03
Yes
No
Yes
特殊コードに変換
S06
文字表示情報の付加
S07
S04
改行キー？
No
入力バッファ更新
入力画面への表示反映
S08
Yes
入力終了
S09
S101
S10
パスワード一致？
No
S11
警告メッセージを表示
Yes
S13
警告メッセージ表示回数？
1回、2回
S12
オペレーティングシステムを起動させる
3回
S14
パソコンの電源オフ

【図４】


S01
オペレータがパソコンの電源オン
S100
特殊コードを含むパスワード入力
S101
S20
修理機能選択の状態信号が含まれる？
No
パスワード再入力
OS起動
電源オフ
Yes
S102
キーコードからなるパスワードと特殊コードからなるパスワードを分離
S21
特殊コードからなるパスワードに一致する修理機能を選択
S22
キーコードからなるパスワードを修理機能のパスワードとする
S23
S24
修理機能のパスワードが一致するか？
Yes
No
修理ユーティリティの起動
S25
電源オフまたは再起動
S26

【図５】


A
オペレータがパソコンの電源オン
B
オペレータにパスワードの入力を促す
キー入力？
No
Yes
改行キー？
No
入力バッファ更新
入力画面への表示反映
Yes
入力終了
C
パスワード一致？
No
D
警告メッセージを表示
Yes
F
警告メッセージ表示回数？
1回、2回
E
オペレーティングシステムを起動させる
G
3回
パソコンの電源オフ

フロントページの続き

(56)参考文献 特開２００４－０４６６８８（ＪＰ，Ａ）
特開平１１－０３９２６０（ＪＰ，Ａ）
特開２００３－２４８７３５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００　－　２１／２４